UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208

25299 7590 08/16/2006

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/771,472	Applicant(s) CALVIGNAC ET AL.	
	Examiner Ellen C. Tran	Art Unit 2134	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 July 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-20*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Continuation of 11. does NOT place the application in condition for allowance because: no arguments or amendment was presented that overcome the Final Office Action rejection mailed 13 June 2006.

In response to Applicant arguments on page 7, "Applicant respectfully disagrees that these claims are indefinite. Paragraphs [0007] and [0009] of the instant published application No. 2002/0101985 explains that the singe hardware cycle may take several clock cycles or just one clock cycle ... Furthermore, the Examiner has not explained how the use of the term "clock cycle" would render the claims unclear to one having ordinary skill in the art having read the specification" The Examiner maintains that these claims are indefinite and can use Applicant's response as well as language in the claims to clarify why the 112 rejection is maintained, claim 9 states the following "The hardware implementation of a crypto-function recited in claim 1, wherein the one hardware cycle is approximately ten clock cycles". The term approximately is indefinite, the applicant admits a hardware cycle may take several or just one clock cycle but the duration of the clock cycle is not defined 20msec, 30 msec, or 2nsec, further more claim 9 does not define how many clock cycles are in a hardware cycle, rather the claim is indefinite because it indicates a range of clock cycles. Therefore the limitation as such, "clock cycle" (see [0005-0009] fails to establish the meets and bounds of the claimed limitation (see claim 9). Thus the examiner maintains the 112 rejection for at least the reasons stated above, at this time.

In response to Applicant's argument on page 7, "The Examiner asserts that claim 13 is indefinite and does not further limit the invention. Applicant respectfully disagrees that this claim is indefinite. Paragraph [0007] of the instant published application No. 2002/0101985 defines combinational logic as logic functions whose outputs depend solely on their inputs ... having ordinary skill in the art having read the specification". The Examiner disagrees with argument and notes the claim is interpreted in light of the specification. Claim 13 was rejected under 112 2nd, because the inputs are not defined, repeating a phrase in the specification does not make the claim definite, the input is not defined.

In response to Applicant's argument beginning on page 8, Greene fails to teach each and every element of the claims ...Greene does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle ... As explained on paragraph [0005] of the instant published application. Conventional processing of crypto-functions requires many clock and hardware cycles". Examiner notes the Applicant is trying to limit Greene by placing the limitations the application claimed improvement. Examiner disagrees that Greene incorporates any of the noted limitations see col. 4, lines 58-67 "Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit" furthermore the encryption circuit can include numerous cipher stages see col. 5, lines 6-12.

In response to Applicant's argument beginning on page 10, "Furthermore, while the Examiner has specifically pointed to col. 4, line 58 to col. 5, line 13 as disclosing the recited computation ... the noted language is entirely silent with regard to the terms "computational logic" and "crypto-function". Examiner disagrees as interpreted Greene shows these limitations see col. 5, lines 1-24, "computational logic" is interpreted to be equivalent to "Each data stream can include one data block or a sequence of data blocks having a particular order. Each such data block and/or sequence of data blocks will be referred to herein as a "context", note each context incorporates various sequences and order, i.e. computation; "crypto-function" is interpreted to be equivalent to "cipher stage".

In response to "For example, the Examiner is not correct that col. 7, lines 7-21 and col. 7, lines 62 to col. 8, line 4 discloses that the combination logic performs an invertible key dependent round function iterated ... (claim 5)". The Examiner disagrees the invertible key is shown "the encrypted form of data block A1 (designated as E[A1]) is an input that is used together with data block A2 to encrypt data block A2". The scheduler determines how many rounds each key is used.

In response to "Examiner is also not correct that col. 7, lines 7-21 and col. 8, lines 6-32 discloses that the combination logic performs mixing, permutation and key-dependent substitution in each round (claim 6)". The Examiner disagrees again the scheduler determines which key is to be used with each round.

In response to Applicant's argument beginning on page 12, "Examiner is also not correct that col. 7, lines 51-67 discloses that the combination logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation (claim 7)". The Examiner disagrees deciphering by using the same key for encryption is shown, note encryption is used throughout the description but it is understood that "encryption" can include both encryption and decryption, see col. 4, lines 29-31.

In response to Applicant's argument on page 13, "The Examiner is also not correct that col. 5, lines 7-12 discloses that the one hardware cycle is approximately ten cycles (claim 9)". The Examiner disagrees the whole reference should be review and notes see col. 4, line 64 to col. 5, line 12; which notes a cycle can be as small as one clocked cipher stage and that multiple cipher stages can be implemented in parallel.

In response to Applicant's argument beginning on page 13, "Examiner is also not correct that col. 5, lines 7-12 discloses that the hardware implementation of the crypto-function computes an iterated round function in one clock cycle (claim 11)". The reference as a whole should be reviewed one clock cycle can be implemented in one hardware cycle in Greene in addition "iterated round function" are shown in col. 6, lines 58-67.